NISTTech

A Technique for Combinational Circuit Optimization and a New Circuit for the S-Box of Advanced Encryption Standard (AES)

A method to simplifying a combinational circuit

Description

The invention is a two-step technique for combinational circuit optimization. In the first step, the non-linearity of the circuit - as measured by the number of nonlinear
gates it contains - is reduced. The second step reduces the number of gates in the linear components of the circuit.

Applications

- Computing an inverse in a Galois Field, which is a field containing a finite number of elements

Advantages

- The technique can be applied to arbitrary circuits

Abstract

A method of simplifying a combinational circuit establishes an initial combinational circuit operable to calculate a set of target signals. A quantity of multiplication operations performed in a first portion of the initial combinational circuit is reduced to create a first, simplified combinational circuit. The first portion includes only multiplication operations and addition operations. A quantity of addition operations performed in a second portion of the first, simplified combinational circuit is reduced to create a second, simplified combinational circuit. The second portion includes only addition operations. Also, the second, simplified combinational circuit is operable to calculate the target signals using fewer operations than the initial combinational circuit.

Inventors

- Peralta, Rene
- Boyar, Joan

Citations

1. J. Boyar, R. Peralta, A new combinational logic minimization technique with applications to cryptology, Lecture Notes in Computer Science Vol. 6049/2010, 178-189, 2010.

References

- U.S. Patent Application # 20100202605
- Docket: 08-033

Status of Availability

available for licensing

Last Modified: 12/28/2010